ABSTRACT

A system and method for securely exchanging plurality of information items used to generate a plurality of encryption keys used in a public key-and-private key system. In accordance with the principles of the invention, elements of exchanged information items, such as public key and synchronizing indictors are encrypted before the exchange. The information item element is encrypted using an encryption key determined from information items that were previously exchanged. The encryption of information items used to determine subsequent encryption keys provides additional security to the encryption key used in the transmission of informational data as the encrypted elements of the information item must be decrypted before the data message encryption key can be decrypted. The process of exchanging encrypted information items can be repeated until an agreed upon number of encrypting keys is determined.